UNITED STATES DISTRICT COURT

for the

Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

Case No.17-MJ- 509

IN THE MATTER OF THE SEARCH OF THE SEARCH OF:
EMAIL ACCOUNTS: WEKNOW@HOTDAK.NET
KATYJONES76@HOTDAK.NET,
KATYJONES76@MUCHOMAIL.COM. AND
KATYJONES1976@MUCHOMAIL.COM

APPLICATION FOR A SEARCH WARRANT

I, KEVIN PARKER, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York *(identify the person or describe property to be searched and give its location):*

The subject property to be searched: EMAIL ACCOUNTS: **WEKNOW@HOTDAK.NET, ATYJONES76@HOTDAK.NET, KATYJONES76@MUCHOMAIL.COM. AND KATYJONES1976@MUCHOMAIL.COM, as described in Attachment A.**

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: **See Attachment B for the Items to be Seized, all of which are fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030 and 2261A, and all of which are more fully described in the application and affidavit filed in support of this warrant, the allegations of which are adopted and incorporated by reference as if fully set forth herein.**

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- X evidence of a crime;
- X contraband, fruits of crime, or other items illegally possessed;
- X property designed for use, intended for use, or used in committing a crime;
- ___ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of **Title 18, United States Code, Sections 1030 and 2261A,** and the application is based on these facts which are continued on the attached sheet.

__ Delayed notice of 30 days (give exact ending date if more than 30 days) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA KEVIN PARKER, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: January 23, 2017

Judge's signature

City and State: Rochester, New York

HON. JONATHAN W. FELDMAN, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the following email accounts stored at premises owned, maintained, controlled, or operated by Everyone.net, a company located at 892 Ross Drive, Sunnyvale, California.

a. weknow@hotdak.net;

b. katyjones76@hotdak.net;

c. katyjones76@muchomail.com; and

d. katyjones1976@muchomail.com.

ATTACHMENT B

Information to be Seized

Because Everyone.net is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Everyone.net to perform the search would be a burden upon the company. If all Everyone.net is asked to do is produce all the files associated with the account, an employee can do that easily. Requiring Everyone.net to search the materials to determine what content is relevant would add to their burden. Therefore, in order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Everyone.net, to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to Everyone.net, personnel by law enforcement agents. Everyone.net, personnel will be directed to isolate those accounts and files described below;

2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts and/or files described below;

3. The Everyone.net, system administrator will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;

4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant;

5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator and will not further review the original duplicate absent an order of the Court.

I. Information to be disclosed by Everyone.net

To the extent that the information described in Attachment A is within the possession, custody, or control of Everyone.net, Everyone.net, is required to disclose the following information to your Affiant for each account or identifier listed in Attachment A:

a. The contents of all emails stored in the account, including copies of emails sent from the account;
b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any creditor bank account number);
c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
d. All content in the Docs, Calendar, Friend Contacts and Photos areas;
e. Any and all files linked to email accounts of the user; and
f. All records pertaining to communications between Everyone.net or the domain owner (for example hotdak.net), and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by your Affiant

All records or information, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030 (unauthorized computer access and computer-related fraud) and 2261A (stalking), including, but not limited to, for each account or identifier listed on Attachment A, information pertaining to:

a. The contents of any such communications that will assist investigators in ascertaining the nature and scope of the crimes under investigation, the true identity and or location of the subjects and any co-conspirators, the names, addresses, and any disposition of the proceeds of the crimes under investigation, including;
b. Records relating to who created, used, or communicated with the account or identifier;
c. Records pertaining to accounts held with companies providing Internet access or remote storage of tangible items, documents, data, or storage media;

d. Records relating to ownership or use of phones including passwords, pins, and encryption keys necessary to access such devices and/or applications on devices (e.g., voicemail)

e. Records, including, but not limited to, video files, audio files, images, stored messages, recordings, books, documents, and cached web pages relating to either stalking or computer intrusion scheme;

f. Records reflecting the communications with or the existence, identity, travel, or whereabouts of, any co-conspirators;

g. Any other identifying information associated with the user of the account (financial information, employment information, patterns of behavior, etc.);

h. Records of activities or usage relating to the operation or ownership of any computer hardware, software, storage media, Internet / online accounts, or data (such as usernames, passwords, telephone records, and notes).

ADDENDUM TO SEARCH WARRANT
SEARCH OF COMPUTERS

1. The computer or electronic media search authorized by this warrant shall be completed within 60 days from the date of the warrant unless, for good cause demonstrated, such date is extended by Order of this Court.

2. In conducting the search authorized by this warrant, the government shall make reasonable efforts to utilize computer search methodology to search only for files, documents or other electronically stored information which are identified in the warrant itself.

3. Should the government not locate any of the items specified in the warrant (or other fruits, contraband, instrumentalities, or property subject to forfeiture) within the authorized search period (including any extensions granted), the government shall return the computer or electronic media to the owner.

4. In any circumstance not covered by paragraph three (3) above, upon completion of the search, the government, upon request of the owner of the computer, shall promptly return to the owner of the computer copies of all files and documents requested and specified by the owner, excluding any items or files seized pursuant to the warrant or other fruits, contraband, instrumentalities or property subject to forfeiture.

5. If electronically stored data or documents have been identified by the government pursuant to this warrant, or other fruits, contraband, instrumentalities or property subject to forfeiture, the government may retain the original hard drive or other data storage mechanism pending further order of this Court. The retention of the original hard drive or other data storage mechanism does not relieve the government of its obligation to return to the owner of the computer files, documents or other electronically stored information identified in paragraph (4) above.

6. Nothing in this warrant shall limit or prevent the government from retaining the computer or electronic media as fruits, contraband or an instrumentality of a crime or commencing forfeiture proceedings against the computer and/or the data contained therein. Nothing in this warrant shall limit or prevent the owner of the computer or electronic media from (a) filing a motion with the Court pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure for the Return of Property or (b) making a request of the government to return certain specified files, data, software or hardware.

7. Should there be a dispute or question over ownership of any computer or any electronically stored data or documents stored therein, the government shall promptly notify this Court so that such dispute or question can be resolved.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF EMAIL ACCOUNTS: WEKNOW@HOTDAK.NET, KATYJONES76@HOTDAK.NET, KATYJONES76@MUCHOMAIL.COM, AND KATYJONES1976@MUCHOMAIL.COM	Case No. _____ **[UNDER SEAL]**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kevin Parker, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since September, 2011. I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York. As part of the Cyber Squad, I work on investigations relating to criminal and national security cyber intrusions. I have gained experience through training and everyday work related to these types of investigations. During my tenure with the FBI I have also worked on other types of investigations including counterintelligence and counterterrorism. I am familiar with fundamental operations of the internet, hardware, software, and the communication protocols across each. Experience with similar investigations and working with other FBI Special Agents and computer forensic professionals has expanded my knowledge of internet communications and, more specifically, internet based obfuscation techniques. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, mobile phones and tablets, and electronically stored information, in conjunction with various criminal investigations.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

3. I make this affidavit in support of an application for a search warrant authorizing the search of email accounts controlled by the Service Providers known as Everyone.Net, located at 892 Ross Drive, Sunnyvale, California 94089.

4. The email accounts and the information to be searched are described in the following paragraphs and in Attachments A and B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Service Providers to disclose to your Affiant records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including contents of communications.

5. I respectfully submit that probable cause exists to believe that evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030 (unauthorized computer access and computer-related fraud) and 2261A (stalking) (the target offenses) will be found in the accounts:

a. weknow@hotdak.net;

b. katyjones76@hotdak.net;

c. katyjones76@muchomail.com; and

d. katyjones1976@muchomail.com.

6. In my training and experience, I have learned that Everyone.Net is the email provider for the email domains hotdak.net and muchomail.com. Everyone.Net is a company that offers email services to small businesses by providing the necessary hosting infrastructure. As such, these small businesses will most likely have a unique email domain name (for example hotdak.net) even though they are hosted on Everyone.Net infrastructure. Everyone.Net provides Internet electronic mail (email) access to the public, and that stored electronic communications, including opened and unopened email for subscribers, may be located on the computers owned or leased by Everyone.Net. Accordingly, this application for a search warrant seeks authorization solely to search the computer accounts and/or files following the procedures set forth herein.

7. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, information provided by other law enforcement agents, and private companies. Because this affidavit is submitted for the limited purpose of obtaining search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to search the above referenced facilities.

RELEVANT STATUTES

8. This investigation concerns alleged violations of: 18 U.S.C. § 2261(A) – Stalking and 18 U.S.C. § 1030 – Fraud and Related Activity in Connection with a Computer.

a. 18 U.S.C. § 2261(A) prohibits a person (a)(2) from using the mail, any interactive computer service or electronic communication service with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person and that

such use places that person in reasonable fear of the death of or serious bodily injury or causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person.

b. 18 U.S.C. § 1030 prohibits a person from (a)(2) intentionally accessing a computer without authorization or exceeds authorized access and thereby obtains (C) information from any protected computer.

PROBABLE CAUSE

9. In or about November 2016, the Buffalo FBI met with the New York State Police regarding an ongoing computer intrusion and stalking investigation. Initial discussions identified a Rochester, New York based female (hereinafter, the "victim") that has been targeted throughout 2016 through the use of a variety of internet based mediums. Following the end of a relationship with William Rosica, the suspected "target user"[1], the victim began receiving harassing text messages, phone calls, and emails. The communications slowly escalated in both content and obfuscation techniques. In addition, the victim's work email account and online medical system (University of Rochester's MyChart) had numerous unauthorized access attempts. Investigation results to date have shown the subject target user to use the TOR network in conjunction with other obfuscation web sites and email providers.

10. In February 2016, the victim ended a three-year relationship with Roscia. Following the end of the relationship the victim and Rosica engaged in conversations

[1] The affidavit references William Rosica both as "Rosica" and the "target user". The affidavit will refer to the subject as "Rosica" during instances that Rosica had direct and identifiable communication with the victim. The affidavit will refer to Rosica as the "target user" during instances that Rosica concealed his identity through the use of the Tor Network.

regarding the ending of the relationship. On March 3, 2016, Rosica emailed the victim with the following, "... Please consider speaking with me and allowing me the chance to make things clearer and more right with you. I know you are very upset. ...Being too quick to anger and too quick to accuse is NOT what I want to do ever again..." On March 23, 2016, the victim received an anonymous text message which stated it was from 'trustmeiknow@yahoo.com' and included the message: "I have already provided him with all of the information he needs to know how you played him. And you wonder why you have no friends?"

11. Also on March 23, 2016, the victim received a text message from 'anonymous@textem.net' with the message: 'I think he knows how you played him. Arguing and fighting to throw him off. All while you were setting up with someone else?'

12. Based on the Affiant's training and expertise combined with research associated from this investigation, your Affiant believes that 'trustmeiknow@yahoo.com' is not a real email address and was entered within a website advertising free text messaging. The website www.textem.net markets free text messaging services; any user with access to the internet can navigate to this website and enter a recipient's phone number, sending email address (optional), recipient mobile carrier, and message content. The Affiant performed a text message test on December 2, 2016, using the fake email address of 'abc@yahoo.com' and message content of 'Test'; the message was received on the Affiant's cellular phone and appeared to have been sent by 'abc@yahoo.com.' It is your Affiant's belief that text messages referenced throughout the remainder of this affidavit utilize the same or similar services and

that the email addresses provided are not real nor used in traditional email communications by the target user.

13. On April 17, 2016, Rosica emailed victim and stated the he had also been the target of harassing emails and text messages. The content of the email included the following, "I have had enough. All hours of the day, night, middle of the night. If you know who is doing this please have them stop! The last two came from lmino@yahoo.com. I have my number blocked from that one site. Thank u. Includes six attachments of screen shots taken from a mobile phone screen. First image, from trustmeiknow@yaho..., series of incoming text messages: "wake up and realize what it is", "whatever you do do not trust her she is lying bigtime you fool", "has she told you yet?", "she needs to tell you something soon she is hiding something from you run!!". Second image, from lmino@yahoo.com, series of incoming text messages: "HA HA", "FUCK OFF!". Third image, from iamonit@yahoo.com, series of incoming text messages: "she is not telling you everything. There is something going on you need to know about", "don't say you weren't warned", "sorry to trouble you but she is up to something you really need to know about", "when are you going to learn your lesson??? She is not telling you everything!", "shes lying to you". Fourth image, from iamonit@yahoo.com, series of incoming text messages: "Has she told you yet? She needs to tell you something", "when will you learn?", "you need to wake up", "wake up idiot!". Fifth image, from iamonit@yahoo.com, series of incoming text messages: "why are you wasting your time? She is a liar", "are you frustrated yet?", "you have been played oh so well", "she has serious issues you need to know about!!", "shes got someone over there right now". Sixth image, from iamonit@yahoo.com, series of incoming text messages: "you missed out on the good

information you fool", "you are an idiot. You deserve what you get.", "haven't you figured it out yet?", "what a jerk off you are! She is playing you!!!!!!!!", "fuck you", "dumb fuck"."

14. On or about May 22, 2016, the victim stated that she broke off all communications with her Rosica. The victim told the FBI this was one of the first milestones in the evolution of the target user; one of the first turning points when she noticed the harassment and communications become more aggressive and technically sophisticated.

15. On June 3, 2016, the victim received an email sent from Rosica, the content of the email included: "I take responsibility for anything I have said or done that was misguided based on rumor, innuendo or from misplaced anger." "I am sorry for the document I left with you because in NO WAY did I intend to imply anything from it other than your own concerns, that you have shared with me, regarding your thyroid issues. I NEVER meant that the entire document pertained to you and I should have been clearer about that. I really thought I was trying to help. Please believe that!" The document referenced by Rosica was a research paper titled, "The Thyroid and the Mind and Emotions/Thyroid Dysfunction and Mental Disorders" and was written by a Professor of Psychiatry with the University of Toronto.

16. On July 16, 2016, the victim received an email sent from Rosica, the content of the email included: "I remain deeply concerned for your well being whether you agree with that or not. I will repeat this forever I DO NOT think you are crazy, psycho or mental... I wish I could have handled the paperwork thing differently."

17. On September 6, 2016, the victim received multiple automated text messages from AT&T (Victim's cellular phone provider). The text messages provided the following, "AT&T Free Msg: Your User ID is lansing862904suv. Wireless number 585-635-9226 can also be used to log in. Did not request? 800.ATT.2020." Based on the Affiant's training and expertise, this text message represents the attempted and potentially successful access of the victim's AT&T online account.

18. On September 7, 2016, Rosica sent the victim an email with the following, "I am on the phone with the fraud department at Verizon. Since 4:05 p.m. yesterday, I have had 17 attempts into my Verizon account. The password keeps getting reset. I have also had 24 attempts into my AOL account. Three step verification is already in place. I have had 2 attempts into my Google account (which is odd because only a handful of people know that I even use that account). Two step verification is in place. "Katy Jones" has now sent me 216 emails! One better than the other. She's one busy girl. This is all legitimate and NOT bullcrap! I have saved every message from Verizon, AOL, and Gmail. I am working diligently to find out the perpetrator and I am very close to going public with this and filing a police report if it does not stop! I am pissed, exhausted and frustrated. I do not want anyone knowing my business (which could also drag you into this). Please, if you know who is doing this, tell them to stop now! Enough is enough!"

19. The Katy Jones identified in the email from Rosica is a reference to the email accounts katyjones76@yandex.com and katyjones76@muchomail.com; further, Rosica is referencing emails he received with alleged details the victim's activities. The victim told the

FBI that all activities referenced in the emails were false. Based upon emails sent from the victim to the FBI, who had received them directly from Rosica, the Katy Jones email accounts sent the following (not exhaustive):

a. July 10, 2016: katyjones76@yandex.com to Rosica; "she [referring to the victim] goes by your [referring to Rosica] house all the time she is waiting for you to screw up she has been talking a lot about your job [referring to Rosica's job as a police officer]"

b. July 11, 2016: katyjones76@yandex.com to Rosica; "shes been asking questions and shes been going by your house ask your neighbors!"

c. July 12, 2016: katyjones76@yandex.com to Rosica; "she is on your street right now"

d. July 21, 2016: katyjones76@muchomail.com to Rosica; "your job cant protect you"

e. July 23, 2016: katyjones76@muchomail.com to Rosica; "lawn looks good whos in your garage??" On July 23, 2016, Rosica forwarded this email to the victim and stated the following, "This is the approximate 58th email since about two weeks ago (this one with a picture). I have spent the last few nites camped out in my front and side yard. There is no one in my garage. I really hope this stops soon as if I didn't already have enough to worry about. I hope all is well with you."

20. Yandex is a Russian multinational technology company specializing in Internet-related services and products. Yandex operates the largest search engine in Russia

with about 60% market share in that country; it is the Affiant's opinion that Yandex would be comparable to Google (and Gmail) in the United States.

21. A subpoena return for the email account katyjones76@muchomail.com identified the following subscriber data: Name: Katy Jones, 123 Main St, Dallas, TX 75189, DOB: 1/1/76, Join Date: 7/21/2016, Total Logins: 171, and Last Login on 9/12/2016 from IP address: 91.121.230.209. An open source lookup of the IP address identified a TOR exit node.

22. On September 8, 2016, three attempted login attempts were made into the victim employer's email system. The IP Addresses used for the attempted access were from TOR Network exit nodes. September 8, 2016, represents the first date known in the investigation where the target user attempted access into the victim employer's email account.

23. Throughout the month of September 2016 additional text messages were received from AT&T with similar attempted access messages as identified above. On or about the middle of September, the victim changed cellular phone numbers and online accounts; soon after switching the victim received the same AT&T automated text messages with the new online ID. Additionally, multiple additional attempts to access the victim's employer email account were made, and all were made from TOR exit nodes.

24. On September 18, 2016, katyjones1976@muchomail.com sent an email to Rosica with the following, "this is [victim's] new car parked at her ex-husband's house on

[address] have her explain why she is at her ex's house when she has made it know he was abusive to her shes even helping him do yard work in her kaki shorts and grey t-shirt this was taken on sunday 9 18 aroun [*sic*] 1pm".

25. On September 18, 2016, Rosica forwarded the email above from Katy Jones and sent an email to the victim with the following, "Whoever Katy Jones is, and as annoying as she has been, her information is accurate. How can you deny this??... When you decided to start sending things back to me with my name on them in July, that's when I suspected you had someone else. We started talking again and I begged for you to tell me the truth and you kept lying, as is evident now. You knew I knew. I felt sorry for you because I thought you were going to kill yourself again like you did several years ago. Remember when you were in-patient psych for downing all of those phenobarbital pills??... Better yet, maybe your son needs to know just how psycho you are... Did you bring Gypsy with you to [victim's ex-husband's] today or did you leave her home in the crate again? ...Both doctors were right about you—Borderline Personality Disorder along with Mania and Depression (although you only ever admitted to the depression). You are pathetic, PSYCHO, a LIAR, and the MOST untrustworthy person I have ever met... What would your son think of his mother being suicidal? That is where you are headed. You have created such messes in your life that you will end up having no other option."

26. A subpoena return for the email account katyjones1976@muchomail.com identified the following subscriber data: Name: Katy Jones, 123 Rochester, NY 14604, DOB:

1/1/76, Join Date: 9/23/2016, Total Logins: 29, and Last Login on 9/23/2016 from IP address: 89.163.237.45. An open source lookup of the IP address identified a TOR exit node.

27. On September 22, 2016, the victim stated she agreed to meet, in person, with her Rosica. According to the victim, Rosica stated, "I am at a crossroads. Either I let you walk away and we live our separate lives or short of killing you, I destroy every aspect of your life. You tell me what I should do." The victim stated her request was to be left alone and walk away. The victim identified this meeting as another milestone further increasing the intensity of harassing contact and technical sophistication.

28. On or about October 6, 2016, the IT Manager for the victim's employer, was contacted by the employer's office manager. The office manager informed the IT manager that a user at the company had their email hacked. The IT manager checked access logs, enabled two-factor authentication for the victim, and changed passwords. The IT manager extracted available logs for the previous 180 days and voluntarily provided those to the NY State Police. Following the involvement of the FBI, the NY State Police then provided the FBI those historic logs. The FBI's review of the alleged hacking indicated that, with a high level of confidence, no unauthorized access was obtained for the period of activity provided; all unauthorized activity was only attempted and either failed at an invalid password or stopped after a challenge question. Based upon the FBI's review of the logs, the total number of unique unauthorized attempted access logins was 142 times, beginning September 8 and ending on October 20 (on or about when the logs were extracted).

29. On October 16, 2016, the victim received a text message from email account 'sycamoreneighbor@yahoo.com' with the message: 'when sneaking around at night and switching and hiding vehicles, please remember to shut the lights off in your house so you don't waste electricity'. The victim's home residence is off a street with the name Sycamore. Based on the Affiant's training and expertise, and the investigation to date, your Affiant believes the email address to not be an authentic Yahoo address and was only used to harass the victim.

30. On October 19, 2016, the victim received a text message from email account 'flatchest@yahoo.com' with the message: 'watch your speed Winton or Monroe tonight? what time will you be at keiths or is he coming over tonight?' Based on the Affiant's training and expertise, and the investigation to date, your Affiant believes the email address to not be an authentic Yahoo address. Further, your Affiant believes the content of the message was used to scare the victim into believing she is being followed and that the sender knows her route home.

31. On October 25, 2016, the victim received four separate text messages with references to assisting in suicide. From email address 'lightsoutonsycamore@yahoo.com', message: http://www.mysticmadness.com/7-easiest-and-best-ways-to-commit-suicide.html. From email address 'halfpynt72@gmail.com', message: http://www.cracked.com/article_15658_the-ten-minute-suicide-guide..html. From email address 'trailertrashliar@yahoo.com', message: http://www.alexshalman.com/2008/08/05/10-simple_-ways-to-commit-suicide/. From

email address 'loser@yahoo.com', message: http://www.insidermonkey.com/blog/7-easiest-painless-ways-of-killing-yourselves-quickest-360388/.

32. On October 26, 2016, the victim received six unique text messages from Google with a verification code. Based on the Affiant's training and expertise, your Affiant believes these text messages were initiated based upon unauthorized access attempts into the victim's personal email account.

33. On October 29, 2016, the victim received numerous text messages. A portion of those text messages provide medical characteristics of individuals with personality disorder (for example, 'people with personality disorder are also usually very impulsive, oftentimes demonstrating self-injurious behaviors'). The remaining portion of emails reference encouraging the victim to commit suicide. Text message from 'halfpynt72@gmail.com' to victim, message: trailer trash lying cheating psycho u ruin everything you touch liar liar psycho liar cheater cheater liar psycho go take some pills lots of them. Text message from 'halfpynt72@gmailc.om' to victim, message: watching the move [*sic, intended to be movie*] "me before you" twice in one week is a good sign your thinking of killing yourself again good for you do it right this time psycho. Text message from '5857336606@txt.att.net' to victim, message: watching the move [*sic*] "me before you" twice in one week is a good sign your thinking of killing yourself again good for you do it right this time psycho. Text message from 'halfpynt72@gmail.com' to victim, message: watch more suicide related movies then take some more of your pills. Text message from 'email@addthis.com' to victim, message: SUBJ: 99 Little Known Facts about suicide MSG: watch more suicide related movies and tell people

you are not psycho and crazy take plenty more pills you are out of your mind and a liar. Text message from 'noreply@txt2day.com' to victim, message: SUBJ:Sent by IP 46.166.188.209 MSG: interesting movie selections more suicide flicks?

34. On October 30, 2016, the victim received an email from weknow@hotdak.net with the message: "anyone(everyone) knows what a liar you are you cant ever keep youre stories straight with your neighbors no need to hide in any of the garages you park in we know what you do and when you do it you get no sympathy from us you ruined our quiet neighborhood with your trailer park antics." This was the first email the victim received from the email account weknow@hotdak.net.

35. A subpoena return for the email account weknow@hotdak.net identified the following subscriber data: Name: all knowing, 123 Main St, Rochester, NY 14605, DOB: 1/1/76, Join Date: 10/30/2016, Total Logins: 124, and Last Login on 12/18/2016 from IP address: 51.15.36.187. An open source lookup of the IP address identified a Europe based cloud storage and data provider.

36. On November 27, 2016, the victim received an email from weknow@hotdak.net with the message: "youre little "lies" werent so little after all it has unraveled all this mess people must know what a true skank you are lying filthy cheating trailer trash skank with a grossly fat ass and ankles as big as stumps are you tired yet of ruining others? Seek help or eat pills or both!"

37. On November 27, 2016, the victim received an email from katyjones76@hotdak.net with the message, "since you like lying and cheating so much why dont you ask trailer boy mechanic who (girl) was at his house while you were in Carolina lets see if he can lie as good as you he parked her in his left garage your still the skaniest [*sic*] of them all ps a few more people are blind copied in with each email." This is believed to be the first email associated with the name Katy Jones that was under the hotdak.net email domain. The Government believes this is an indicator that all Katy Jones and weknow@hotdak.net accounts are associated with the same user.

38. On November 30, 2016, two attempts were made to remotely access the online University of Rochester MyChart account containing medical information for the victim. The attempts were identified via automated Login ID recovery emails sent to victim's personal email account. An interview of the victim stated she did not initiate the unauthorized attempted access but she did change her password after learning of the attempts.

39. On December 7, 2016, the victim received a phone call from Walgreens stating her prescription was ready for pick-up. After speaking with the pharmacist, victim stated that she had previously cancelled all her auto-refill prescriptions but for some reason this one was not cancelled. After picking up her prescriptions the evening of December 7, 2016, the victim received an email from weknow@hotdak.net with the message: bout time you picked up youre psyche pills at drug store youre driving is not great either hurry home so you can go to trailvervile how does it feel deep in youre mind to know you are a skank liar? .... don't be

surprised how many people know all of this... a suicidal skank liar so many people know that now..."

40. Also on December 7, 2016, two individuals at the victim's employer received emails from weknow@hotdak.net. The emails were sent to the Managing Partner and Office Operations Manager. Content of the email stated: "you need to look closer at her do not let her fool you if you talk to the right people they will tell you what you need to hear you should read some of the emails she has sent about youre firm ask the right people and you will find the truth do not be fooled!"

41. An interview with the victim's pharmacy identified a pattern of anonymous and fake phone calls inquiring about the victim's medications. The employees at the pharmacy have documented phone calls on September 26, 2016, October 20, 2016, seven times on December 1, 2016, December 2, 2016, December 3, 2016, December 4, 2016, December 6, 2014, December 14, 2016, December 15, 2016, twice on December 16, 2016, December 29, 2016, four times on December 30, 2016, January 2, 2017, and January 4, 2017.

42. On December 13, 2016, weknow@hotdak.net sent a second email to the victim employer's managing partner and operations manager. The content of the message included: "[victim] is creating this drama because she is mad about her bonus you should here her bad mouth you both shes hoping all this attention will make you feel sorry for her go look at her emails and see what she has sent out about both of you talk to the other firms where holly is known as the "C" word according to [victim] john is a "dirty cheating lawyer" the girls at these other firms can confirm this she has serious mental issues."

43. On December 14, 2016, the victim refilled a prescription through a Walgreens automated tool and 14 minutes later received an email from weknow@hotdak.net with the message: "you have 2 new psyche meds waiting for you hopefully this batch of pills will fix youre illness if not just take the whole bottle are these antiskank pills? ...another person found out today what a lying skank you are".

44. On December 15, 2016, weknow@hotdak.net sent a third email to the victim employer's operations manager. The content of the message included: "check her emails she continues to shit talk you she has talked to a lot of girls from other firms about you she is looking for a new job everyday on work time she calls [Managing Partner first name] a crook and you a "C" word every change she gets she is already crying about her bonus dont let her fool you she creates drama so people will feel sorry for her she makes shit up all the time she is poison she has serious mental issues and is heavily medicated do not let her fool you if you want more info let me know she loves ruining lives."

45. On December 21, 2016, the victim received an email from weknow@hotdak.net with the message: "youre plans for a new job will not go well a certain note about you has been circulated to the right people and they wont even touch youre resume they too know what a lying untrustworthy skank you are you have sent out some interesting emails over the last few months and youre boss now is not to happy be careful of the smiling face that says "dont worry [victim] we believe you" you will be out of a job soon enough you filthy lying skank"

46. On December 23, 2016, the victim received an email from weknow@hotdak.net with the message: "...give the world a great present and finish what you started 30 years ago..." The Affiant believes this is a reference to the victim overdosing a prescription medication resulting in a serious medical event for the victim.

47. On January 2, 2017, the victim reported that the target user called Walgreens impersonating the victim's primary care physician. The FBI interviewed the pharmacist who took that call and confirmed an attempted call from someone who claimed they were with the 'Office of [the victim's doctor]' and wanted to know details of medication for the victim. The caller hung up after the pharmacist asked for more information at the doctor's office.

48. On January 5, 2017, the victim received an email from weknow@hotdak.net with the message: "...Attempt suicide lately skank?..."

49. On January 5, 2017, an email was sent from iama.skank@yandex.com to the victim's place of employment. The recipients of the email were the Managing Partner of the Law Firm, the Office Operations Manager, and Office Manager. All individuals are in the direct chain of command over the victim. The message of the email was: "did [victim] tell you how pissed she was about her bonus? she mentioned both of you by name with some of her "friends" at other firms she doesnt even try to hide it [character return] according to [victim] she does more work than both of you combined, [Managing Partner] is having an affair with some new lawyer and [Employee Name] is the office snitch [victim] has serious issues she should not be trusted go back and look at her outgoing emails before she deletes

them [character return] if she denies any of this let me know and i will give you the names of the other people she has spoken to at the different firms she has serious psyco issues she has been making up stories about what is "happening" to her so she can get attention dont fall for it shes on psyco meds right now"

50. For the purposes of this Search Warrant, the Affiant has only included text messages and emails relevant to establish probable cause for this affidavit. The victim is also the recipient of ongoing anonymous phone calls, at times as frequent as one a minute at her place of employment. The victim's family has received similar anonymous phone calls to include parents, sibling, and ex-husband. The victim has stated that almost every evening her cable box is restarted without her initiating the action.

51. Based on my knowledge and experience, as well as the facts previously stated, there is probable cause to believe that a single target user is in control of the email accounts weknow@hotdak.net, katyjones76@hotdak.net, katyjones76@muchomail.com, katyjones1976@muchomail.com, katyjones76@yandex.com, and iama.skank@yandex.com. Further, there is probably cause to believe the above email accounts were used in facilitation of the target offenses.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

52. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device

performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

53. I have had training in the investigation of computer-related crimes. Based on my training, and experience, I know the following:

f. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;

g. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and

h. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email

server may allow users to post and read messages and to communicate via electronic means.

54. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

55. The ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, Internet Protocol addresses, and other information both in computer data format and in written record format.

56. "TOR" or "TOR Network", also known as the "Onion Router", is a network of computers designed to facilitate anonymity. Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible

Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org. The Tor software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP back through that Tor exit node IP. In that way, using the Tor network operates similarly to a proxy server – that is, a computer through which communications are routed to obscure a user's true location.

BACKGROUND REGARDING EVERYONE.NET

57. Based on my training and experience, I have learned the following about Everyone.Net

i. Everyone.net provides Software as a Service (SaaS) messaging for service providers and businesses worldwide;

j. Everyone.net services over 300,000 domains worldwide;

k. Everyone.net is considered an electronic communications service ("ECS") provider because it provides its users access to electronic communications service as defined in Title 18,United States Code, Section 2510(15). Internet users sign-up for a subscription service from small businesses that use Everyone.Net to host infrastructure required to support the email needs of small business clients. The individual small businesses request email subscribers to provide basic information such as name, gender, address, zip code, and other personal / biographical information. However, typically these small businesses do not authenticate the information provided;

l. Everyone.Net maintains electronic records pertaining to the small businesses for which are their clients. The records include account access information, email transaction information, and account application information;

m. Any email that is sent from an Everyone.net customer is stored in the individual email subscriber's "mail box" on Everyone.net infrastructure until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by the service provider. If the message is not deleted by the subscriber, the account is below the storage limit, and the subscriber accesses the account periodically, that message could remain on Everyone.net's infrastructure indefinitely;

n. An Everyone.net customer could theoretically store files, including emails and image files, on servers maintained and/or owned by Everyone.net; and

o. Emails and image files stored on an Everyone.net server by a subscriber may not necessarily also be located in the subscriber's home computer. The subscriber may store emails and/or other files on the Everyone.net server for which there is insufficient storage space in the subscriber's own computer or which the subscriber does not wish to maintain in his or her own computer. A search of the subscriber's home, business, or laptop computer will therefore not necessarily uncover files the subscriber has stored on the Everyone.net servers.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

58. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Everyone.net to disclose to your Affiant copies of the records and other information (including the content of communications) particularly described in Section I in the Attachment B annexed hereto. Because Everyone.net is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Everyone.net to perform the search would be a burden upon the company. If all Everyone.net is asked to do is produce all the files associated with the account, an employee can do that easily. Requiring Everyone.net to search the materials to determine what content

is relevant would add to their burden. Upon receipt of the information described in Section I in the Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

59. Based on my training and experience, and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that in the email accounts located on computer systems owned, maintained, and/or operated by Everyone.net, located at 892 Ross Drive, Sunnyvale, California, there exists evidence, contraband, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1030 (unauthorized computer access and computer-related fraud) and 2261A (stalking). I therefore respectfully request that the Court issue a search warrant directed to Everyone.net for the email accounts identified in Attachment A for information described in Attachment B.

60. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States ... that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

61. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

62. Because this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto could jeopardize the progress of the investigation. Disclosure of the search warrant at this time could jeopardize the investigation by giving the targets an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Respectfully submitted,

Kevin Parker, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on January 23, 2017

HONORABLE JOHN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE